Слюсарев Артём Андреевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Усков Арсений Николаевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Кухтин Владимир Олегович, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Шамчиков Антон Андреевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Черников Фёдор Сергеевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

АВТОМАТИЗАЦИЯ ЦИФРОВЫХ РАССЛЕДОВАНИЙ: СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ И ПОДХОДЫ

Аннотация. Актуальность данного исследования обусловлена стремительным расширением цифровых инфраструктур и соответствующим ростом числа киберинцидентов, которые формируют всё более крупные и сложные массивы данных, требующие оперативного криминалистического анализа. По мере усложнения кибератак традиционные ручные методы расследования перестают справляться с объёмом и динамикой угроз, что

приводит к задержкам, неполноте анализа и повышенным рискам для организаций. Эти вызовы делают развитие и внедрение автоматизированных средств цифрового расследования не просто полезным, но необходимым.

В данном контексте цель статьи заключается в исследовании ключевых направлений автоматизации цифровых расследований, рассмотрении наиболее эффективных современных инструментов и платформ, а также анализе методологических подходов, повышающих точность, скорость и надёжность обработки цифровых доказательств. Путём анализа возможностей и преимуществ автоматизированных систем статья подчёркивает их возрастающую роль в построении устойчивых и эффективных процессов кибербезопасности.

The relevance of this study is driven by the rapid expansion of digital infrastructures and the corresponding rise in cyber incidents, which generate increasingly large and complex datasets requiring timely forensic analysis. As cyberattacks become more sophisticated, traditional manual investigation methods struggle to keep pace, resulting in delays, incomplete analyses, and higher risks for organizations. These challenges make the development and adoption of automated digital investigation tools not only beneficial but essential.

In this context, the article aims to explore key trends in the automation of digital investigations, examine the most effective modern tools and platforms, and analyze methodological approaches that enhance the precision, speed, and reliability of digital evidence processing. By outlining the capabilities and advantages of automated systems, the article highlights their growing importance in building resilient and efficient cybersecurity processes.

Ключевые слова: кибербезопасность, цифровая криминалистика, автоматизация расследований, SIEM, SOAR, машинное обучение, кибератака.

Keywords: cybersecurity, digital forensics, investigation automation, SIEM, SOAR, machine learning, cyberattack.

Литература

- Иванов Д.Д. Применение цифровой криминалистики в современных расследованиях и анализе данных / Иванов Д.Д. // Вестник науки. 2023. № 4. С. 78–88.
- Исаков А.А. Искусственный интеллект и расследование киберпреступлений / Исаков А.А. // Вестник науки. 2023. С. 45–52.
- Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 / Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. // Труды СПИИРАН (Информатика и автоматизация). 2016. № 4 (47). С. 5–27.
- Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 / Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. // Труды СПИИРАН (Информатика и автоматизация). 2016. № 6 (49). С. 208–225.
- Штеренберг С.И., Данилова Ю.С. Разработка методики внедрения и выявления эффективности SIEM-системы / Штеренберг С.И., Данилова Ю.С. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 40–45.

Literature

- Ivanov D.D. Application of digital forensics in modern investigations and data analysis / Ivanov D.D. // Vestnik Nauki (Science Bulletin). 2023. No. 4. P. 78–88.
- Isakov A.A. Artificial intelligence and the investigation of cybercrimes / Isakov A.A. // Vestnik Nauki (Science Bulletin). 2023. P. 45–52.
- Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analysis of security event correlation methods in SIEM systems. Part 1 / Fedorchenko

A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. // SPIIRAS Proceedings. 2016. No. 4 (47). P. 5–27.

- Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analysis of security event correlation methods in SIEM systems. Part 2 / Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. // SPIIRAS Proceedings. 2016. No. 6 (49). P. 208–225.
- Shterenberg S.I., Danilova Y.S. Development of a methodology for implementation and evaluation of SIEM-system effectiveness / Shterenberg S.I., Danilova Y.S. // Bulletin of Saint Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2020. No. 3. P. 40–45.

Введение

Цифровая криминалистика традиционно опиралась на ручные методы анализа данных, что делало расследования трудоёмкими и длительными. Современная цифровая среда характеризуется динамичной инфраструктурой, большим количеством логов и разнообразием цифровых артефактов, что требует новых подходов.

Автоматизация цифровых расследований обеспечивает скорость и точность обработки информации, снижает влияние человеческого фактора, стандартизирует процессы анализа и повышает достоверность получаемых результатов. В условиях роста числа киберинцидентов автоматизация становится не просто полезной, а критически необходимой.

Основные задачи автоматизации цифровых расследований

Автоматизация цифровых расследований решает несколько ключевых задач. Прежде всего, она позволяет собирать цифровые доказательства из распределённых систем, облаков, локальных машин и сетевых устройств с минимальным участием эксперта, при этом обеспечивая сохранность и целостность данных.

Следующая задача – предварительный анализ данных, который ускоряется за счёт алгоритмов корреляции, машинного обучения и правил обнаружения. Эти методы позволяют быстро выявлять подозрительные события и сокращают время обработки больших объёмов логов.

Кроме того, автоматизация помогает построению временной линии инцидента на основе разнородных данных, что облегчает понимание последовательности событий. Корреляция информации из различных источников позволяет получать комплексную картину инцидента, особенно при расследовании многоуровневых атак. В завершение, системы обеспечивают автоматическое формирование отчётов, что ускоряет процесс документирования и повышает стандартизацию результатов расследования.

Современные инструменты автоматизации

На рынке цифровой криминалистики можно выделить несколько групп инструментов:

- SIEM-системы (Security Information and Event Management)

SIEM-платформы собирают события безопасности, выполняют корреляцию данных и уведомляют аналитиков о подозрительных событиях. Наиболее популярные решения: Splunk, IBM QRadar, ArcSight, Elastic SIEM.

- SOAR-платформы (Security Orchestration, Automation and Response)

SOAR-системы автоматизируют реакции на инциденты и позволяют запускать предопределённые сценарии. Среди них: Palo Alto Cortex XSOAR, Splunk SOAR, IBM Resilient.

Функции этих платформ включают автоматическую блокировку IP, сбор логов, проверку файлов на вредоносность и интеграцию с другими системами безопасности, что снижает нагрузку на аналитиков.

- Машинное обучение и искусственный интеллект

ML-модели позволяют выявлять аномальное поведение, обнаруживать скрытые связи между событиями и классифицировать вредоносную активность. Нейросетевые алгоритмы особенно эффективны при анализе больших массивов логов и сетевого трафика.

- Автоматизированные криминалистические инструменты

Специализированные решения для цифровой криминалистики включают в себя следующие инструменты:

- Autopsy – обработка больших объёмов данных;
- Magnet AXIOM – автоматическая корреляция артефактов из разных источников;
- FTK (Forensic Toolkit) – ускорение анализа цифровых носителей.

Подходы к автоматизации расследований

Современные системы автоматизации разрабатываются с учётом нескольких принципов:

- Во-первых, модульность и масштабируемость обеспечивают возможность горизонтального расширения ресурсов для обработки больших объёмов данных.
- Во-вторых, инфраструктура как код (IaC) позволяет фиксировать состояние систем и инфраструктуры в момент инцидента, что облегчает расследование.

Кроме того, автоматизация цепи цифровых доказательств обеспечивает соблюдение принципа Chain of Custody без ручного вмешательства. Не менее важна интеграция с облачными сервисами (AWS CloudTrail, Google Cloud Logging, Azure Monitor), которая позволяет получать доступ к событиям и логам в автоматическом режиме и проводить расследование в облачной среде.

Заключение

Автоматизация цифровых расследований становится стратегически важным элементом информационной безопасности. Она сокращает время анализа инцидентов, повышает точность оценки последствий и улучшает качество реагирования на угрозы.

Перспективы развития включают усиление роли искусственного интеллекта, создание полностью автономных систем расследования и внедрение предиктивной аналитики, способной предотвращать инциденты на ранних этапах.